

☐ UNCLASSIFIED ☒ INTERNAL ☐ CONFIDENTIAL ☐ SECRET

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

## ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Markings Requirements for Office of Logistics (AIUO)

FROM:

[Redacted]

OL Markings Task Force  
Representative

EXTENSION

NO.

DATE

TO: (Officer designation, room number, and building)

DATE

RECEIVED

FORWARDED

OFFICER'S  
INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1. [Redacted] 7 NOV 1978  
DDA Representative to E.O.  
12065 Markings Task Force

AP

2.

3.

DDA RMO

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

**SECRET**

6 NOV 1978

25X1

MEMORANDUM FOR: [REDACTED]

DDA Representative to E.O. 12065  
Markings Task Force

25X1

FROM: [REDACTED]

OL Markings Task Force Representative

SUBJECT:

Markings Requirements for Office of Logistics (AIUO)

REFERENCE:

Memo dtd 25 Aug 78 to [REDACTED] DDA  
Rep/OL fm [REDACTED] Same subj.

25X1

25X1

1. (U) Through discussions with Logistics Divisions and Staffs, I find that classifications and/or controls OL is presently using are in adherence to existing regulatory procedures. In the following paragraphs I have mentioned specific items that reflect OL requirements, as effected by Executive Order 12065. I have also included several questions pertaining to forms classification that should be resolved by the Markings Task Force prior to the implementation of new markings on 1 December 1978.

2. (U) As a result of the review of Logistics forms, and in concurrence with cognizant offices, I am preparing necessary paperwork to delete certain forms and change or remove some classifications. In addition, due to lack of space, several of our forms will restrict placement of the new classification markings directly at the bottom or top of the form. However, there is sufficient area in the body of each form to place these markings. Please advise me if, under the new policy, this placement is not appropriate.

**SECRET**

25X1

OL 8 - 5074

~~SECRET~~

Subject: Markings Requirements for Office of Logistics (AIUO)

3. (S) For your information, the following Logistics forms will retain their present classification because content would contain sensitive information:

a. Form 794 - Vehicle status (remain SECRET) - This form contains Agency vehicle characteristics, vehicle location; [redacted] stations, license and body numbers, names of case officers in either true or pseudonym, and, if applicable, project names or cryptonyms. *Blank or filled in* 25X1

b. Form 2109 - Monthly Supply Operations Report (remain CONFIDENTIAL WHEN FILLED IN) - When completed this document contains the amount of square feet of various types of ordnance materiel stored in certain buildings, at the Logistics [redacted] 25X1

25X1

[redacted] 25X1

d. Form 3953 - Resource Allocation Sheet (remain CONFIDENTIAL) - This form is preprinted with all organizational functions including the Intelligence Community Staff.

4. (AIUO) The below listed forms are preprinted with a caution requiring secure storage in the field. While these forms are not classified, they are peculiar to the Agency and issued to [redacted] I believe for this reason the DDO requested they be controlled in this manner. I will therefore, need a reading on whether this marking should or can remain on these forms before any action on my part to remove or change this control marking. 25X1

*Issued to be controlled or to be controlled*

- a. Form 88 - Requisition for Materiel and/or Services
- b. Form 1330 - All Purpose Property Transaction Record
- c. Form 1331 - Materiel Record Card

~~SECRET~~

Subject: Markings Requirements for Office of Logistics (AIUO)

5. (C) We have re-evaluated the classification of the forms noted below, but require that each be classified with internal control markings if the present "ADMINISTRATIVE INTERNAL USE ONLY" (AIUO) marking is repealed. I will, therefore, require a reading on this subject from the Markings Task Force:

a. Form 3540 - Competitive Evaluation Criteria (AIUO)

b. Form 3540a - Competitive Evaluation Criteria (AIUO)

c. Form 3848 - Project Pace Registration Form (CONFIDENTIAL)

d. Form 2216 - Procurement Order for MIL or FEDSTRIP (FOR OFFICIAL USE ONLY).

6. (U) Lastly, OL generates a number of classified computer reports annually. All reports are received from the computer with the classification printed both top and bottom of each page. I have discussed, with our Systems Analysis Branch, the feasibility of programming the declassification markings data into each scheduled report, including individual queries, so that this information would then be automatically printed on each page at the time the report is run. Before we can undertake this reprogramming however, I will require the declassification markings format, when available.

7. (U) Please let me know if additional information or clarification is required. I can be contacted at 3G31  Building, extension

25X1

25X1

SECRET

STAT

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

A

## 11. IDENTIFICATION AND MARKINGS

All national security information classified by the Agency shall be identified as to the authority for its classification, and the level and duration thereof.

## a. OVERALL AND PAGE MARKINGS

- (1) The highest classification level of information contained within a document shall be typed or stamped at the top and bottom of the outside front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Each interior page shall be typed or stamped at the top and bottom either according to the highest classification of the content of the page, including the designation "Unclassified" when appropriate, or according to the overall classification of the document.

- DC (D/H) This paragraph is being rewritten.*
- (2) Only the designations Top Secret, Secret, or Confidential may be used to identify classified information. Markings such as "For Official Use Only" and "Limited Official Use" may not be used in conjunction with classification designations, e.g., "Conference Confidential" or "Agency Confidential".
- why not define what a page will use?*

## b. CLASSIFICATION AUTHORITY AND DURATION MARKINGS

- (1) Originally Classified Documents. In addition to the overall document classification, the following shall be shown on the face of paper copies of originally classified documents at the time of origin:

- (a) The date and office of origin.
- (b) The identity of the classifier.
- (c) The date or event for declassification or review.
- (d) If the document is classified for more than six years:
  - (1) The identity of the Top Secret classifier who authorized the prolonged classification.
  - (2) The reason the classification is expected to remain necessary despite the passage of time.

EXAMPLE: The following marking should be applied to the lower right corner on the face of each originally classified document to identify the information specified in b. through d. above.

ORIGINAL CL BY. 1/  
☐ DECL ☐ REVW ON 2/  
EXT BYND 6 YRS BY 3/  
REASON 4/

1/ Insert the authorized classifier's employee number or other identifier approved by the Agency Security Classification Officer. If the classifier does not have the requisite classification authority but is officially acting in the absence of an official who does have such authority, insert the classifier's employee number followed by the position number of the absent official, e.g., 012345 for PG12.

2/ Check the appropriate box to indicate whether the document is to be automatically declassified or reviewed for declassification and insert the specific date (day, month, year) or event for such action to occur, e.g., 01JAN96.

3/ If the date or event for declassification or review exceeds six years from the date of the document, insert the employee number or other identifier approved by the Agency Security Classification Officer of the Top Secret classifier who is authorizing the extended classification--even if this is the same identifier inserted in 1/.

4/ Cite the applicable subparagraph from paragraph 10d of this regulation which explains the reason classification is expected to remain necessary for the extended period.

- (2) Derivatively Classified Documents. In addition to the overall document classification, the following shall be shown on the face of paper copies of derivatively classified documents at the time of origin:
- (a) The date and office of origin.
  - (b) The identity of the derivative classifier.
  - (c) The source from which the classification is derived.
  - (d) The date or event for declassification or review, carried forward from the classification source.

EXAMPLE: The following marking should be applied to the lower right corner on the face of each derivatively classified document to identify the information specified in b. through d. above.

DERIVATIVE CL BY 1/  
☐ DECL ☐ REVW ON 2/  
DEATED FROM 3/

1/ Insert the derivative classifier's employee number or other identifier approved by the Agency Security Classification Officer.

2/ Insert the date (day, month, year) or event for automatic declassification or review for declassification carried forward from the classification source, e.g., 01JAN96. If the classification is derived from more than one source, insert the latest date or event. (See paragraph of this regulation for further instructions on declassification dates for derivatively classified information.)



DRAFT COPY

3/ Cite the source document or the classification guide (by guide and item number) from which classification is derived, e.g., Memo from AB to D/CD dated 1 Jan. 78, Subj: Class Markings; (Guide Number) C9b3.2. If classification is derived from more than one source, insert "multiple". In this case, the identification of each source must be shown on the originator's file copy of the document.

c. AUTOMATIC DOWNGRADING MARKING

If automatic downgrading is appropriate and can be predetermined, or is prescribed by a classification guide or source document, the following marking will be stamped or typed on the face of classified documents in addition to the classification authority and duration marking.

"Downgrade to \_\_\_\_\_ on \_\_\_\_\_"

## d. PORTION MARKING

- (1) Each classified document shall indicate which paragraphs or other portions, including subjects and titles, are classified and which are unclassified. The intent is to eliminate uncertainty as to which portions of a document contain information that must be protected, and to facilitate excerpting and declassification review. The symbol, "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, or "(U)" for Unclassified, will be placed immediately following the portion of text to which it applies. Non-textual portions of a document--such as photographs, graphs, charts, and maps--will be marked in a readily discernible manner, as will their captions. If the name of the signer of a document is classified, the typed name will be followed by the appropriate classification symbol.
- (2) Subjects and titles should be selected so as not to require classification. When a classified subject or title must be used, a short title or other unclassified identifier should be assigned to facilitate receipting and reference. If a short title is assigned, it will consist of the first letter of each word in the subject or title and appear in parentheses immediately preceding the classification marking. For example:

Subject: This is a Confidential Subject (T-I-A-C-S) (C)

- (3) If individual portion marking is impracticable, the document must contain a description sufficient to identify the information that is classified and the level of such classification. This may be done by including a statement as the last paragraph of the document or as a footnote or postscript, e.g., "Paragraphs 1, 2, and 4 are Secret, all others Unclassified". If all portions of a document are classified at the same level, this may be indicated either by marking each portion or by including a statement to this effect, e.g., "All paragraphs above are Confidential".
- (4) Waivers from the portion marking requirement may be granted only by the Director of the Information Security Oversight Office. Requests for waivers from Agency components must be submitted to ISAS/RAB for approval by \_\_\_\_\_, and forwarding to ISOO. Such requests must include:
  - (a) identification of the information or classes of documents for which such waiver is sought;

- (b) a detailed explanation of why the waiver should be granted;
- (c) the office's best judgement as to the anticipated dissemination of the information of class of documents for which waiver is sought; and
- (d) the extent to which the information subject to the waiver may form a basis for classification of other documents.

e. ADDITIONAL MARKINGS(1) Restricted Data or Formerly Restricted Data

Classified information containing Restricted Data or Formerly Restricted Data as defined in the Atomic Energy Act of 1954, as amended, shall be marked as prescribed by the Department of Energy.

(2) Intelligence Sources and Methods Information

Classified information involving intelligence sources or methods will be prominently marked:

"Warning Notice - Intelligence Sources and Methods Involved"

This marking may be abbreviated "WNINTEL" in electrical communications, in data processing systems, and for reference purposes.

(3) Foreign Government Information

To assure that foreign government information receives the proper degree of protection, documents containing such data should be marked on their face:

"Contains Foreign Government Information"

This marking may be abbreviated "FGI" in electrical communications, in data processing system, for reference purposes, and for portion (paragraph) marking. For portion marking, "FGI" will follow the classification marking, i.e., (C/FGI), (S/FGI), or (TS/FGI). If the portion marking "FGI" is used, the document need not be marked with the "Contains Foreign Government Information" marking. Where the fact of foreign origin is so sensitive that it must be concealed from normal recipients of the document, the foreign government information markings should not be used and the document should be marked as if it were wholly of U.S. origin--including a duration of classification not to exceed 20 years. In this case, the originator's file copy must indicate the proper duration of classification.

(4) Dissemination and Reproduction Notice

For classified information which the originator has determined is subject to special dissemination and reproduction controls, a statement placing the user on notice of the restrictions shall be included in the text of the document or on its face, e.g., "Reproduction requires approval of originator" or "Further

dissemination only as directed by (insert appropriate office or official)". This form of control should be limited to information that is so sensitive that other means of control would not offer sufficient protection to the information. Offices receiving authorization to reproduce paper copies of such documents must maintain records showing the number and distribution of reproduced copies.

DRAFT COPY

## f. MARKING TRANSMITTAL DOCUMENTS

A transmittal document which is unclassified or classified at a lower level than the information transmitted by it shall indicate both its own classification and the highest classification of the information transmitted. Type or stamp at the top and bottom of each page of the transmittal document the highest classification designation of the transmitted information. At the lower right corner on its face, type or stamp:

"Unclassified when Detached from Enclosure"

or

"(Classification) When Detached from Enclosure"

In the case where the transmittal document is itself unclassified, no classification authority and duration marking should appear.

## g. MARKING FORMS

- (1) Only the specific classification markings that apply to each copy of a form may appear thereon. "Check boxes" to select from preprinted alternative classifications may not be used. Preprinted annotations such as "Secret when filled in" may not be used unless approved in each case by the Agency Security Classification Officer, ISAS/BDA.
- (2) All classified forms must indicate the classification authority and duration information specified in paragraph b. above. To conserve space, the abbreviations in paragraph h. below (Marking Electrically Transmitted Documents) may also be used on forms. Where possible, these markings should be placed in the lower right corner of the form. The classification of the majority of forms will be derived from classification guides. Thus, on most forms, the preprinted "Classification Authority and Duration Line" (CDL) would contain the following derivative classification markings:
  - (a) DCL or RVW \_\_\_\_\_ - (either the date (day, month, year) or event the form will be automatically declassified or the date or event the form will be reviewed for declassification as determined from the classification guide or source document, e.g., 01JAN96.)
  - (b) DRV \_\_\_\_\_ - (identity of the source from which the classification and its duration is derived, i.e., the classification guide and item number, the identity of the source document, or the word "Multiple" if there is more than one source.)
  - (c) BY \_\_\_\_\_ - (derivative classifier's employee number or other identifier approved by the Agency Security Classification Officer.)

A preprinted CDL on a form will normally appear, then, as:

☐ DCL ☐ RVW \_\_\_\_\_ DRV \_\_\_\_\_ BY \_\_\_\_\_

OR

☐ DCL ☐ RVW \_\_\_\_\_  
|←-DRV \_\_\_\_\_ BY \_\_\_\_\_

RECORDS AND CORRESPONDENCE

HUB ☐  
DRAFT COPY

STAT

(NOTE: The CDL must also identify the classifier's office and the date the classification action took place if it is not readily evident from the content of the form.)

- (3) On forms in which the preprinted information is itself classified, the appropriate classification level, authority, and duration will be prescribed by the originator at the time the form is developed.
- (4) Existing stocks of forms may be used until depleted, or until 1 December 1979, whichever is sooner. During this period, the preprinted marking IMPDET will equate to "Review on (date 20 years after date form is filled in)". Anyone filling in a form that contains preprinted classification markings must line through any markings that do not apply to the completed form. When forms are reprinted, overprinted, or revised for any reason, they must be changed to comply fully with the prescribed marking requirements.

DRAFT COPY

## h. MARKING ELECTRICALLY TRANSMITTED DOCUMENTS

- (1) To facilitate the efficient use of electronic transmission systems, abbreviations will be used within the message text to indicate the classification authority and duration (see paragraph b. above). These abbreviations, as listed below, will normally be entered as the last line or paragraph of the text as the "Classification Authority and Duration Line" (CDL). (Examples of the use of the abbreviations follow in paragraph h.(2)).
- (a) RVW - review for declassification on (date or event document will be reviewed for declassification.)
- (b) DCL - declassified on (date or event document will be automatically declassified.)
- (c) DRV - derived from (identity of the source from which the classification and its duration is derived, i.e., the classification guide and item number, the identity of the source document, or the word "MULTIPLE".)
- (d) BY - derivative classification determined BY (derivative classifier's employee number or other identifier approved by the Agency Security Classification Officer.)
- (e) ORG - original classification authority is exercised by (authorized classifier's employee number or other identifier approved by the Agency Security Classification Officer.)
- (f) EXT - extension of classification beyond 6 years by (employee number or other identifier approved by the Agency Security Classification Officer of the Top Secret classifier who is authorizing the extended classification. Used only when original classification authority is exercised and the date for automatic declassification or review for declassification exceeds six years.)
- (g) RSN - reason for extension of classification (used only when original classification authority is exercised and the date for automatic declassification or review for declassification exceeds six years.)

DRAFT COPY

- (h) DNG - downgraded on (date or event when the document will be automatically downgraded. Determined either by the classification guide or, when original classification authority is exercised, by the classifier.)
  - (i) OFF - office originating the message (used only when the office of origin will not otherwise be evident from the transmitted message.)
- (2) To demonstrate the use of the above abbreviations in the CDL, assume that today's date is 01 January 1981, that the classifier's employee number is 011111, and that:

- (a) classification guide "C9b3.2" states that the information in the message will be reviewed for declassification in 20 years.

RVW 01JAN01 DRV C9B3.2 BY 011111

- (b) classification guide "B8a2.1" states that the information in the message will be automatically declassified in 15 years.

DCL 01JAN96 DRV B8A2.1 BY 011111

- (c) original classification authority is exercised and the date for review for declassification is more than six years (in this example, 20 years).

RVW 01JAN01 ORG 011111 EXT 022222 RSN

- (d) original classification authority is exercised and the date for automatic declassification is more than six years (in this example, 15 years).

DCL 01JAN96 ORG 011111 EXT 022222 RSN

- (e) original classification authority is exercised and the date for review for declassification is less than six years (in this example, five years).

RVW 01JAN86 ORG 011111

- (f) original classification authority is exercised and the date for automatic declassification is less than six years (in this example, five years).

DCL 01JAN86 ORG 011111

(NOTE: Field originated electrically transmitted documents need not include the "BY", "ORG" or "EXT" items if the Chief of Station/Base is the classifier.)

- (3) As with other classified documents, electrically transmitted documents must be portion (paragraph) marked (see paragraph d above). If all portions of the message are classified at the same level, this may be indicated either by marking each portion or by inserting the appropriate classification level following the CDL. For example, if all portions of the document in paragraph h(2)(a) above were classified Confidential, the portion marking requirement would be satisfied by:

RVW 01JAN01 DRV C9B3.2 BY 011111 ALL CONFIDENTIAL

- (4) Where required, additional markings such as WNINTEL and FGI will be entered in the next line after the address/addrressor lines (see paragraph e above).

DRAFT COPY

## i. MARKING MATERIAL OTHER THAN DOCUMENTS

The classification and associated markings on material other than documents shall be placed by conspicuously stamping, tagging, or other means. If the material cannot be marked, written notification of the security classification and associated markings must be furnished to any recipients of the material.

100-6527  
10-4-78

THE WHITE HOUSE  
WASHINGTON

September 29, 1978

MEMORANDUM FOR:

Dr. James B. Rhoads  
Acting Chairman  
Interagency Classification  
Review Committee

SUBJECT: Implementing Directive for  
Executive Order 12065 on  
National Security Information

The draft implementing directive for Executive Order 12065 on National Security Information and the comments of the ICRC, submitted with your letter of September 19, 1978, have been reviewed, and further revisions have been made. The attached directive, as revised, is approved for issuance and publication.

  
Zbigniew Brzezinski

Enclosure

INFORMATION SECURITY OVERSIGHT OFFICE

DIRECTIVE No. 1

CONCERNING

NATIONAL SECURITY INFORMATION

This Directive is issued pursuant to the provisions of Section 6-204 of Executive Order 12065. The purpose of the Directive is to assist in the implementation of Executive Order 12065, and users of the Directive shall refer concurrently to the Executive Order for guidance.

TABLE OF CONTENTS

Section I.	ORIGINAL CLASSIFICATION:	
A	Definition	2
B	Classification Authority	2
C	Request for Classification Authority	3
D	Record Requirements	3
E	Classification Procedure	3
F	Foreign Government Information	3
G	Standard Identification and Markings	4
H	Additional Markings Required	9
I	Abbreviations	10
Section II.	DERIVATIVE CLASSIFICATION:	
A	Definition	11
B	Responsibility	11
C	Marking Derivatively Classified Documents	12
D	Classification Guides	13
Section III.	DECLASSIFICATION AND DOWNGRADING:	
A	Record Requirements	14
B	Declassification Policy	14
C	Systematic Review for Declassification	14
D	Procedures for Mandatory Declassification	14
	Review	18

		2
Section IV.	SAFEGUARDING:	
A	General	22
B	General Restrictions on Access	22
C	Access by Historical Researchers and Former Presidential Appointees	23
D	Dissemination	23
E	Accountability Procedures	23
F	Storage	24
G	Transmittal	28
H	Loss or Possible Compromise	31
I	Destruction	31
Section V.	IMPLEMENTATION AND REVIEW: Challenges to Classification	32
Section VI.	GENERAL PROVISIONS:	
A	Notification	32
B	Posted Notice	32
C	Downgrading, Declassification, and Upgrading Markings	33
D	Combat Operations	33
L	Publication and Effective Date	34

#### I. ORIGINAL CLASSIFICATION

A. Definition. "Original classification" as used in the Order means an initial determination that information requires protection against unauthorized disclosure in the interest of national security, and a designation of the level of classification.

(1)\*

B. Classification Authority. In the absence of an authorized classifier, anyone designated to act in that person's absence may exercise the classifier's authority. (1-204)

\*Parenthetical references are to related Sections of Executive Order 12065.

C. Request for Classification Authority. Requests for original classification authority for agencies not listed in Section 1-2 of the Order shall be submitted to the President through the Information Security Oversight Office. Requests shall include: (1) the designation of the officials for whom or positions for which authority is sought, (2) the level of authority requested, and (3) the justification for such requests, including a description of the type of information that is anticipated to require original classification. (1-2)

D. Record Requirements. Agencies and officials granted original classification authority pursuant to Section 1-2 of the Order shall maintain a current listing, by classification designation, of individuals to whom or positions to which original classification authority has been delegated. (1-2)

E. Classification Procedure. Except as provided in Section 1-303 of the Order, the fact that the information concerns one or more of the qualifying criteria or categories of information shall not create any presumption as to whether the information meets the damage tests. (1-302 and 1-303)

F. Foreign Government Information.

1. Identification. "Foreign government information" is:

a. Information provided to the United States by a foreign government or international organization of governments in the

expectation, express or implied, that the information is to be kept in confidence; or

b. Information produced by the United States pursuant to a written joint arrangement with a foreign government or international organization of governments requiring that either the information or the arrangement, or both, be kept in confidence. Such a written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record. (1-303 and 6-103)

2. Duration of Classification. Unless the guidelines developed pursuant to Section 3-404 of the Order or other guidelines prescribe dates or events for declassification or for review for declassification:

a. Foreign government information shall not be assigned a date or event for automatic declassification unless such is specified or agreed to by the foreign government or international organization of governments.

b. Foreign government information classified after the effective date of the Order shall be assigned a date for review for declassification up to thirty years from the time the information was classified or acquired. (1-402 and 3-404)

G. Standard Identification and Markings. At the time of original classification, the following shall be shown on the

face of paper copies of all classified documents:

1. Identity of Classifier. The identity of the classifier, unless also the signer or approver of the document, shall be shown on a "classified by" line; e.g., "Classified by John Doe" or "Classified by Director, XXX." (1-501(a))

2. Date of Classification and Office of Origin. The date and office of origin on a document at the time of its origination may be considered the date of classification and identification of the office of origin. (1-501(b))

3. Date or Event for Declassification or Review. The date for automatic declassification or for declassification review shall be shown on a "declassify on" or a "review for declassification on" line; e.g., "Declassify on 1 November 1984." "Declassify on completion of state visit." or "Review for declassification on 1 November 1998." (1-501(c))

4. Downgrading Markings. When it is determined (e.g., in a classification guide) that a classified document should be downgraded automatically at a certain date or upon a certain event, that date or event shall be recorded on the face of the document; e.g., "Downgraded to Secret on 1 November 1990" or "Downgraded to Confidential on 1 December 1985." (1-5)

5. Identity of Extension Authority. The identity of the official who authorizes a date for declassification or for review for declassification that is more than six years beyond the date of the document's classification shall be shown on the document, unless that official also is the classifier, signer, or approver of the document. This marking shall be shown substantially as follows: "Extended by (Insert name or title of position of agency head or Top Secret classification authority)." (1-502)

6. Reason for Extension. When classification is extended beyond six years, the reason shall be stated on the document either in narrative form or by reference to an agency regulation that states the reason for extension in narrative form. The reason shall be shown substantially as follows: "Reason for extension: (State reason or applicable reference)." (1-502)

7. Overall and Page Marking of Documents. The overall classification of a document shall be marked, stamped, or affixed permanently at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Each interior page of a classified document shall be marked or stamped at the top and bottom either according to the highest classification of the content of the page, including

the designation "Unclassified" when appropriate, or according to the highest overall classification of the document. In any case, the classification marking of the page shall not supersede the classification marking of portions of the page marked with lower levels of classification. (1-501(d))

8. Subjects and Titles. Whenever practicable, subjects and titles shall be selected so as not to require classification. When the subject or title is classified, an unclassified identifier may be assigned to facilitate receipting and reference. (1-5)

9. Mandatory Portion Marking. Classifiers shall identify the level of classification of each classified portion of a document (including subjects and titles), and those portions that are not classified. Portion marking shall be accomplished by placing a parenthetical designator immediately preceding or following the text that it governs. The symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used for this purpose. If individual portion marking is impracticable, the document shall contain a description sufficient to identify the information that is classified and the level of such classification. A waiver of the portion marking requirement may be granted by the Director of the Information Security Oversight Office. Requests for such

waivers shall be made by the head of an agency or designee to the Director and shall include: (a) identification of the information or classes of documents for which such waiver is sought, (b) a detailed explanation of why the waiver should be granted, (c) the agency's best judgment as to the anticipated dissemination of the information or class of documents for which waiver is sought, and (d) the extent to which the information subject to the waiver may form a basis for classification of other documents. (1-504)

10. Material other than Documents. The classification and associated markings prescribed by this Directive for documents shall, where practicable, be affixed to material other than documents by stamping, tagging, or other means. If this is not practicable, recipients shall be made aware of the classification and associated markings by notification or other means as prescribed by the agency. (1-5)

11. Transmittal Documents. A transmittal document shall indicate on its face the highest classification of the information transmitted by it and the classification, if any, of the transmittal document. For example, an unclassified transmittal document should bear a notation substantially as follows:  
"UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE IS DETACHED." (1-5)

12. Marking Foreign Government Information. ~~Except in those cases where such markings would reveal intelligence information, foreign government information incorporated in United States documents shall, whenever practicable, be identified in such manner as to ensure that the foreign government information is not declassified prematurely or made accessible to nationals of a foreign country without consent of the originator.~~ Documents classified by a foreign government or an international organization of governments shall, if the foreign classification is not in English, be marked with the equivalent United States classification. Foreign government information not classified by a foreign government or an international organization of governments but provided to the United States in confidence by a foreign government or by an international organization of governments shall be classified at an appropriate level and shall be marked with the United States classification accordingly.

(1-5)

H. Additional Markings Required. In addition to the marking requirements in paragraph G, the following markings shall, as appropriate, be displayed prominently on classified information. When display of these additional markings is not practicable, their applicability to the information shall be included in the written notification of the assigned classification. (1-5)

1. Restricted Data or Formerly Restricted Data. For classified information containing Restricted Data or Formerly Restricted Data as defined in the Atomic Energy Act of 1954, as amended, such markings as may be prescribed by the Department of Energy in regulations issued pursuant to the Act shall be applied.

2. Intelligence Sources and Methods Information. For classified information involving intelligence sources or methods:

"WARNING NOTICE - INTELLIGENCE SOURCES AND METHODS  
INVOLVED"

3. Dissemination and Reproduction Notice. For classified information that the originator has determined, pursuant to Section 1-506 of the Order, should be subject to special dissemination or reproduction limitations, or both, a statement placing the user on notice of the restrictions shall be included in the text of the document or on its cover sheet; e.g., "Reproduction requires approval of originator," or "Further dissemination only as directed by (Insert appropriate office or official)." (1-506)

I. Abbreviations. Classified documents that are transmitted electrically may be marked with abbreviations or codes in a single line to satisfy the requirements of each subsection of paragraphs G and H in a manner consistent with economic and

efficient use of electrical transmission systems, provided that the full text represented by each such abbreviation or code and its relation to each subsection of paragraphs G and H is readily available to each expected user of the classified documents affected.

## II. DERIVATIVE CLASSIFICATION

A. Definition. "Derivative classification" as used in the Order means a determination that information is in substance the same as information that is currently classified, and a designation of the level of classification. (2-1)

B. Responsibility. Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form information that is already classified, and of those who apply markings in accordance with instructions from an authorized classifier or in accordance with an authorized classification guide. Persons who apply derivative classification markings should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed the basis for classification. Where checks with originators or other appropriate inquiries show that no classification or a lower classification than originally assigned is appropriate, the derivative document shall be issued as unclassified or shall be marked appropriately.

C. Marking Derivatively Classified Documents. Paper copies of derivatively classified documents shall be marked at the time of origination as follows:

1. The classification authority shall be shown on a "classified by" line; e.g., "Classified by (Insert identity of classification guide)" or "Classified by (Insert source of original classification)." If the classification is derived from more than one source, the single phrase "multiple sources" may be shown, provided that identification of each such source is maintained with the file or record copy of the document; (2-102(c))
2. The identity of the office originating the derivatively classified document shall be shown on the face of the document; (2-102)
3. Dates or events for declassification or review shall be carried forward from the source material or classification guide and shown on a "declassify on" or "review for declassification on" line. If the classification is derived from more than one source, the latest date for declassification or review applicable to the various source materials shall be applied to the new information; (2-102(c))
4. The classification marking provisions of Section I.G. 7 through 9 and I.G. 12 are also applicable to derivatively classified documents; (2-102(c))

5. Any additional marking under Section I.H. of this Directive appearing on the source material shall be carried forward to the new material when appropriate; (2-102(c)) and

6. Any abbreviation or code permitted under Section I. I. of this Directive may be applied to derivatively classified documents.

D. Classification Guides.

1. Requirements. Classification guides issued pursuant to Section 2-2 of the Order shall:

a. Identify the information to be protected, using categorization to the extent necessary to ensure that the information involved can be identified readily and uniformly; (2-201)

b. State which of the classification designations (i.e., Top Secret, Secret, or Confidential) applies to the information; (2-201)

c. State the duration of classification in terms of a period of time or future event. When such duration is to exceed six years, the reason for such extension shall be provided in the guide. However, if the inclusion of classified reasons would result in a level of classification for a guide that would inhibit its desirable and required dissemination, those reasons need be recorded only on or with the record copy of the guide; (2-201) and

d. Indicate how the designations, time limits, markings, and other requirements of the Order and this Directive are to be applied, or make specific reference to agency regulations that provide for such application. (2-201)

2. Review and Record Requirements. Each classification guide shall be kept current and shall be reviewed at least once every two years. Each agency shall maintain a list of all its classification guides in current use. (2-2)

### III. DECLASSIFICATION AND DOWNGRADING

A. Record Requirements. Agencies and officials granted original classification authority pursuant to Section 1-2 of the Order shall maintain a record of individuals or positions designated as declassification authorities pursuant to Section 3-103 of the Order. (3-103)

B. Declassification Policy. In making determinations under Section 3-303 of the Order, officials shall respect the intent of the Order to protect foreign government information and confidential foreign sources. (3-303)

C. Systematic Review for Declassification.

1. Systematic Review Guidelines.

a. U.S. Originated Information. Systematic review guidelines shall be kept current through review at least every

the Archivist of the United States. (3-402)

b. Foreign Government Information. Within one year after the effective date of the Order, heads of affected agencies shall, in consultation with the Archivist and in accordance with the provisions of Section 3-404 of the Order, develop systematic review guidelines for thirty-year old foreign government information. These guidelines shall be kept current through review by agency heads at least once every two years, unless earlier review for revision is requested by the Archivist of the United States. A copy of these guidelines and any revisions thereto shall be furnished to the Information Security Oversight Office. Upon request, the Department of State shall provide advice and such assistance as is necessary to effect foreign government coordination of the guidelines. (3-404)

2. Systematic Review Procedures.

a. Scheduling for Systematic Review. Classified non-permanent records that are scheduled to be retained for more than twenty years need not be systematically reviewed but shall be reviewed for declassification upon request. Within sixty days of the effective date of the Order, heads of agencies and officials designated by the President pursuant to Section 1-2 of the Order shall direct that all classified records twenty years old or older, whether held in storage areas by the

agency or in Federal records centers, be surveyed to identify those that require scheduling for future disposition. Such scheduling shall be accomplished within two years of the effective date of the Order. (3-401)

b. Extending Classification After Review.

(1) Foreign Government Information. Agency heads listed in Section 1-2 and officials designated by the President pursuant to Section 1-201 of the Order may extend the classification of foreign government information beyond 30 years, but only in accordance with Sections 3-3 and 3-404. This authority may not be delegated. ~~When classification is extended beyond 30 years, a date no more than ten years later shall be set for declassification or for the next review.~~ Subsequent reviews for declassification shall be set at no more than ten year intervals. (3-404)

(2) ~~Waivers of the ten-year review.~~ Heads of agencies listed in Section 1-2 and officials designated by the President pursuant to Section 1-201 of the Order may request from the Director of the Oversight Office a waiver of the ten-year review requirement for both U.S.-originated and foreign government information. Such requests shall include a personal certification by the agency head that the classified information for which the waiver is sought has been systematically reviewed as required, and that a definitive date for declassification could not be determined. Waivers should not be requested unless

the results of the review have established an identifiable need to continue classification for a period in excess of twenty additional years. Each request shall include a recommended date or event for subsequent review or automatic declassification. (3-401)

c. Assistance to the Archivist.

(1) ~~He shall select, assign, and designate experienced personnel to assist the Archivist of the United States in the systematic review of twenty year-old U.S.-originated information and twenty year-old foreign government information~~ accessioned into the National Archives of the United States. Such personnel shall:

(a) Provide guidance and assistance to National Archives employees in identifying and separating documents and specific categories of information within documents that are deemed to require continued classification; and

(b) Submit to the head of the agency recommendations for continued classification that identify documents or specific categories of information so separated.

(2) The head of the agency shall then make the determinations personally and in writing required under Section 3-401 of the Order as to which documents or categories of information require continued protection. The agency shall inform the Archivist of the United States of this determination. (3-4)

d. Special Procedures. Special procedures for systematic review and declassification of classified cryptologic information and classified information concerning the identities of clandestine human agents promulgated in accordance with the provisions of Section 3-403 of the Order shall be binding on all agencies. (3-403)

e. Foreign Relations Series. In order to permit the editors of Foreign Relations of the United States to meet their mandated goal of publishing twenty years after the event, heads of departments and agencies are requested to assist the editors in the Department of State by facilitating access to appropriate classified materials in their custody and by expediting declassification review of items from their files selected for publication. (3-4)

D. Procedures for Mandatory Declassification Review.

1. U.S.-Originated Information.

a. Action on an Initial Request. Each agency shall designate, in its implementing regulations published in the Federal Register, offices to which requests for mandatory review for declassification may be directed. Upon request for declassification pursuant to Section 3-5 of the Order, agencies shall apply the following procedures:

(1) The designated offices shall acknowledge receipt

(2) Whenever a request does not reasonably describe the information sought, the requestor shall be notified that unless additional information is provided or the scope of the request is narrowed, no further action will be undertaken. (3-501)

b. Information in the Custody of and under the Exclusive Declassification Authority of an Agency. The designated office shall determine whether, under the declassification provisions of Section 3-3 of the Order, the requested information may be declassified and, if so, shall make such information available to the requestor, unless withholding is otherwise warranted under applicable law. If the information may not be released in whole or in part, the requestor shall be given a brief statement as to the reasons for denial, a notice of the right to appeal the determination to a designated agency appellate authority (including name, title, and address of such authority), and a notice that such an appeal must be filed with the agency within sixty days in order to be considered. (3-501)

c. Information Classified by Agencies other than the Custodial Agency. When an agency receives a request for information in its custody that was classified by another agency, it shall forward the request to the appropriate agency for review, together with a copy of the document containing the information requested where practicable, and with its recommendation to withhold any of the information where appropriate.

Unless the agency that classified the information objects on grounds that its association with the information requires protection, the agency that received the request shall also notify the requestor of the referral. After the agency that classified the information completes its review (in coordination with other agencies that have a direct interest in the subject matter), a response shall be sent to the requestor in accordance with the procedures described above. If requested, the agency shall also communicate its determination to the referring agency.

(3-501)

d. Action on Appeal. The head of an agency or a designee shall establish procedures to act within thirty days upon all appeals of denials of requests for declassification. These procedures shall provide for meaningful appellate consideration, shall be forwarded to the Oversight Office for review, and shall be published in the Federal Register. In accordance with these procedures, agencies shall determine whether continued classification is required in whole or in part, notify the requestor of the determination, and make available any information that is declassified and otherwise releasable. If continued classification is required under the provisions of Section 3-3 of the Order, the requestor shall be notified of the reasons therefor. If requested, the agency shall also communicate the appeal determination to any referring agency.

(3-5 and 5-404(c))

e. Fees. If the request requires the rendering of services for which fair and equitable fees may be charged pursuant to Title 5 of the Independent Offices Appropriation Act, 65 Stat. 290, 31 U.S.C. 483a (1976), such fees may be imposed at the discretion of the agency rendering the services. Schedules of such fees shall be published in the Federal Register. (3-501)

2. Foreign Government Information. Except as provided hereinafter, requests for ~~creation review~~ for the declassification of classified documents that contain foreign government information shall be processed and acted upon in accordance with the provisions of Section D.1 above. ~~the agency~~

~~receiving the request is the agency that initially received~~

~~or classified the foreign government information. It shall~~

~~determine whether the foreign government information in the~~

~~document may be declassified and released in accordance with~~

~~agency policy or guidance. After consulting with other agencies~~

that have subject matter interest as necessary. ~~the agency~~

~~receiving the request is not the agency that received or~~

~~classified the foreign government information, it shall refer~~

~~the request to the appropriate agency~~ which shall take action

as described above, including its recommendation to withhold

any of the information where appropriate. In those cases where

~~agency policy on guidelines do not apply. Consultation with~~  
~~the original determination through appropriate channels may be~~  
~~available prior to final action on the request.~~ (3-5)

#### IV. SAFEGUARDING

A. General. Information classified pursuant to Executive Order 12065 or prior Orders shall be afforded a level of protection against unauthorized disclosure commensurate with its level of classification. (4-1)

B. General Restrictions on Access.

1. Determination of Need-to-Know. Classified information shall be made available to a person only when the possessor of the classified information establishes in each instance, except as provided in Section 4-3 of the Order, that access is essential to the accomplishment of official Government duties or contractual obligations. (4-101)
2. Determination of Trustworthiness. A person is eligible for access to classified information only after a showing of trustworthiness as determined by agency heads based upon appropriate investigations in accordance with applicable standards and criteria. (4-101)

C. Access by Historical Researchers and Former Presidential Appointees. Agencies shall obtain (1) written agreements from requestors to safeguard the information to which they are given access as permitted by the Order and this Directive, and (2) written consent to the agency's review of their notes and manuscripts for the purpose of determining that no classified information is contained therein. A determination of trustworthiness is a pre-condition to a requestor's access. If the access requested by historical researchers and former Presidential appointees requires the rendering of services for which fair and equitable fees may be charged pursuant to Title 5 of the Independent Offices Appropriations Act, 65 Stat. 290, 31 U.S.C. 483a (1976), the requestor shall be so notified and the fees may be imposed. (4-3)

D. Dissemination.

Except as otherwise provided by Section 102 of the National Security Act of 1947, 61 Stat. 495, 50 U.S.C. 403 (1970 & Supp. V 1975), classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. (4-403)

E. Accountability Procedures.

to receive, transmit, and maintain current access and accountability records for Top Secret information. An inventory of Top Secret documents shall be made at least annually; however, heads of agencies may authorize the annual inventory of Top Secret documents in repositories, libraries, or activities that store large volumes of such information to be limited to documents to which access has been afforded within the past twelve months. The Director of the Oversight Office may grant a waiver with respect to the requirement of an annual inventory for storage systems involving large volumes of information if security measures with respect to such storage systems are adequate to prevent access by unauthorized persons. (4-103)

2. Secret and Confidential. Secret and Confidential classified information shall be subject to such controls and current accountability records as the head of the agency may prescribe. (4-103)

F. Storage. Classified information shall be stored only in facilities or under conditions adequate to prevent unauthorized persons from gaining access to it. (4-103)

1. Top Secret. Top Secret information shall be stored in a GSA-approved, safe-type, steel file cabinet having a built-in,

three-position, dial-type combination lock or within an approved vault, or vault-type room, or in other storage facility that meets the standards for Top Secret established under the provisions of subsection 3 below. In addition, heads of agencies shall prescribe such additional, supplementary controls as are deemed appropriate to restrict unauthorized access to areas where such information is stored. (4-103)

2. Secret and Confidential. Secret and Confidential information shall be stored in a manner and under the conditions prescribed for Top Secret information, or in a container or vault that meets the standards for Secret or Confidential, established pursuant to the provisions of subsections 3 or 4 below. (4-103)

3. Standards for Security Equipment. The General Services Administration shall, in coordination with agencies originating classified information, establish and publish uniform standards, specifications, and supply schedules for containers, vaults, alarm systems, and associated security devices suitable for the storage and protection of all categories of classified information. Any agency may establish more stringent standards for its own use. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above and shall, to the maximum extent practicable, be of the type designated on the Federal Supply Schedule, General Services Administration. (4-103)

4. Exception to Standards for Security Equipment.

a. Secret and Confidential information may also be stored in a steel filing cabinet having a built-in, three-position, dial-type, changeable combination lock, or a steel filing cabinet equipped with a steel lock bar, provided it is secured by a three-position, changeable, combination padlock approved by GSA for the purpose. The storage of Secret information in the steel filing cabinets described above requires the use of such supplementary controls as the head of the agency deems necessary to achieve the degree of protection warranted by the sensitivity of the information involved. (4-103)

b. For protection of bulky Secret and Confidential material (for example, weaponry containing classified components) in magazines, strong rooms, or closed areas, access openings may be secured by changeable combination or key-operated, high-security padlocks approved by GSA. When key-operated padlocks are used, keys shall be controlled in accordance with subsection 6 below. (4-103)

5. Combinations.

a. Equipment in Service. Combinations to dial-type locks shall be changed only by persons having appropriate security clearance, and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination no

longer requires access to the combination, whenever a combination has been subjected to possible compromise, whenever the equipment is taken out of service, and at least once every year. Knowledge of combinations protecting classified information shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information to be stored in the security equipment concerned. (4-103)

b. Equipment Out of Service. When security equipment having a built-in combination lock is taken out of service, the lock shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30. (4-103)

6. Keys. Heads of agencies shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected. Under no circumstances may keys be removed from the premises. They shall be stored in a secure container. (4-103)

7. Responsibilities of Custodians. Persons entrusted with classified information shall be responsible for providing

and for locking classified information in approved security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures that ensure unauthorized persons do not gain access to classified information. (4-103)

8. Inspections. Individuals charged with the custody of classified information shall conduct the necessary inspections within their areas to ensure adherence to procedural safeguards prescribed to protect classified information. Agency security officers shall ensure that periodic inspections are made to determine whether procedural safeguards prescribed by agency regulations are in effect at all times. (4-103)

G. Transmittal.

1. Preparation and Receipting. Classified information shall be enclosed in opaque inner and outer covers before transmitting. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential information shall require a receipt only if the sender deems it necessary. The receipt

shall identify the sender, addressee, and the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Any of these wrapping and receipting requirements may be waived by agency heads under conditions that will provide adequate protection and prevent access by unauthorized persons. (4-103)

2. Transmittal of Top Secret. The transmittal of Top Secret information shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system specially created for that purpose, or over authorized secure communications circuits. (4-103)

3. Transmittal of Secret. The transmittal of Secret material shall be effected in the following manner:

a. The Fifty States, District of Columbia, and Puerto Rico. Secret information may be transmitted within and between the fifty States, District of Columbia, and Puerto Rico by one of the means authorized for Top Secret information, by the United States Postal Service registered mail, or by protective services provided by United States air or surface commercial carriers under such conditions as may be prescribed by the head of the agency concerned. (4-103)

b. Canadian Government Installations. Secret information may be transmitted to and between United States Government and Canadian Government installations in the fifty States, the District of Columbia, and Canada by United States and Canadian registered mail with registered mail receipt. (4-103)

c. Other Areas. Secret information may be transmitted from, to, or within areas other than those specified in subsections a or b above by one of the means established for Top Secret information, or by United States registered mail through Army, Navy, or Air Force Postal Service facilities provided that the information does not at any time pass out of United States citizen control and does not pass through a foreign postal system. Transmittal outside such areas may also be accomplished under escort of appropriately cleared personnel aboard United States Government and United States Government contract vehicles or aircraft, ships of the United States Navy, civil service manned U.S. Naval ships, and ships of U.S. Registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are United States citizens and who are appropriately cleared may be designated as escorts. (4-103)

4. Transmittal of Confidential. Confidential information shall be transmitted within and between the fifty States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories or possessions by one of the means established

for higher classifications, or by United States Postal Service certified, first class, or express mail service when prescribed by an agency head. Outside these areas, Confidential information shall be transmitted only as is authorized for higher classifications. (4-103)

H. Loss or Possible Compromise. Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated by the agency or organization. In turn, the originating agency shall be notified about the loss or compromise in order that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of such a compromise. An immediate inquiry shall be initiated by the agency under whose cognizance the loss or compromise occurred, for the purpose of taking corrective measures and appropriate administrative, disciplinary, or legal action. (4-103)

I. Destruction. Non-record classified information that has served its intended purpose shall be destroyed in accordance with procedures and methods approved by the head of the agency. The method of destruction selected must preclude recognition or reconstruction of the classified information or material. (4-103)

## V. IMPLEMENTATION AND REVIEW

Challenges to Classification. Agency programs established to implement the Order shall encourage holders of classified information to challenge classification in cases where there is reasonable cause to believe that information is classified unnecessarily, improperly, or for an inappropriate period of time. These programs shall provide for action on such challenges or appeals relating thereto within thirty days of receipt and for notification to the challenger of the results. When requested, anonymity of the challenger shall be preserved. (5-404(d))

## VI. GENERAL PROVISIONS

A. Notification. Notification of unscheduled changes in classification or changes in duration of classification may be by general rather than specific notice. (4-102)

B. Posted Notice. If prompt re-marking of large quantities of information would be unduly burdensome, the custodian may attach a change of classification notice to the storage unit in lieu of the marking action otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action, and the storage units to which it applies.

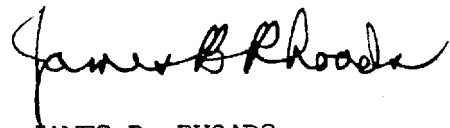
Items permanently withdrawn from such storage units shall be marked promptly in accordance with the marking provisions herein. However, when information subject to a posted downgrading, upgrading, or declassification notice is withdrawn from one storage unit solely for transfer to another, or a storage unit containing such information is transferred from one place to another, the transfer may be made without marking if the notice is attached to or remains with each shipment. (4-102)

C. Downgrading, Declassification, and Upgrading Markings.

Whenever a change is made in the original classification or in the dates of downgrading or declassification of any classified information, it shall be promptly and conspicuously marked to indicate the change, the authority for the action, the date of the action, and the identity of the person taking the action. Earlier classification markings shall be cancelled when practicable. (4-102)

D. Combat Operations. The provisions of the Order and this Directive with regard to dissemination, transmittal, or safeguarding of classified information may be so modified in connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe. (4-103)

E. Publication and Effective Date. This Directive shall be published in the Federal Register. It shall become effective December 1, 1978. (6-204)



JAMES B. RHOADS  
Acting Chairman  
Interagency Classification  
Review Committee

October 2, 1978

PROPOSAL FOR  
WAIVER FROM PORTIONAL MARKING REQUIREMENT

1. An ADP data base will be classified as an entity using criteria in Section 1-3. All reports from a data base will carry the same classification and be marked in accordance with Section 1-501. Text files containing paragraphs that will be used in producing documents must be portionally marked.

2. Computerized data bases contain data that range from unclassified through Top Secret. The resources required to portionally mark each data item, keep such a data element current (the classification of the data changes with circumstance) and to automatically classify reports based on the classification of those data items is substantial. The cost of doing this is not in the public interest.

3. Often data bases include individual items that when processed or reported together have a higher degree of classification. The computer technology is not such that we can identify and program all such relationships so that computer-generated reports using such data can be properly classified. The same determination used in classifying a computer data base is used for classifying reports derived from that data base.

4. Computer reports are generally only disseminated internally to the Agency and they are used for administrative and research purposes.

5. Documents produced using data from a computer data base will be classified under the same criteria as the data base.

~~CONFIDENTIAL~~

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

3 NOV 1978

MEMORANDUM FOR: Chairman, Markings Task Force

25X1 FROM:

DDA Representative, Markings Task Force

SUBJECT: Control Markings

1. The Markings Task Force has been discussing the discontinuation of the control marking, "Administrative - Internal Use Only." The arguments for doing away with it are substantial:

- a. It has been misused a great deal; and
- b. The safeguarding sanctions are not clearly defined.

2. I have discussed the use and need of such a marking with a number of people throughout the DDA. There is a need to protect internal Agency information which if released might be misused or be misleading. These papers include:

- a. Management options and recommendations; and
- b. Administrative planning and procedures.

3. Discussion for the need to have a positive indicator to alert employees that a document contains such information has been lively and interesting. Some of the arguments for and against include:

- a. Some people feel if a piece of paper is not marked, employees will/may take it home and discuss the contents freely.
- b. Unclassified government information doesn't need to be marked as it is U.S. Government property and all employees should be aware of this and handle all such material as prescribed by regulations and law.

UNCLASSIFIED When Separated  
From Enclosure

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

~~CONFIDENTIAL~~

CONFIDENTIAL

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

25X1

c. What about HR [ ] (attached), "Care and Use of Official Data"? This regulation is under review for revision as the current definition of "Official Data" includes all overt material received by the CIA, including the New York Times, library books, etc. Those reviewing the regulation are having problems coming to grips with the definition.

4. In order to provide proper control over Agency internal documents, I suggest we do one of two things:

a. Write a proper definition of "Official Data" and get the regulation out to all employees. If a component is concerned they may indicate on a document "Official Data - Internal Use Only;" or

b. Develop a new control marking for documents which

(1) reflect opinion or recommendations for management policy; or

(2) administrative procedures.

5. The first option appeals as HR [ ] spells out control of information in general. Sanctions are provided whether the information is marked or not.

25X1

6. The second option implies a new marking with a new definition. We suggest "Agency Restricted" as a marking to meet this need. This could be defined as:

Information prepared by Agency personnel or consultants, such as that pertaining to opinions, recommendations, interpretations, plans or internal procedures, the disclosure of which could prejudice, hinder or deter the Agency from carrying out essential management or administrative functions.

7. The intent is (1) to ensure that such information is only released to the public through authorized channels and (2) to provide an environment conducive to the uninhibited exchange of ideas. Sanctions for the improper use of an unclassified document should follow those for unauthorized release. (There is opposition to giving a control marking

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

CONFIDENTIAL

CONFIDENTIAL

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

to documents containing national security information. We have been relying on the classification to control these papers. I submit that even after classifications are no longer valid, the internal nature of some of these documents will remain.)

8. In summary, we need at least <sup>to</sup> provide a positive indicator to control the dissemination of unclassified management information and administrative procedures.

Signed

25X1

Attachment: a/s

cc: DDO/PC  
NFAC/I  
DDS&T  
OGC (J  
DDA/OS  
ISAS/I  
ISAS/I

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

CONFIDENTIAL

SECURITY

**21. CARE AND USE OF OFFICIAL DATA.** All information, classified or unclassified, received, compiled or created by the Central Intelligence Agency (except personal copies of unclassified personnel papers) is official data and is the property of the United States Government.

**a. POLICY**

- (1) All employees are prohibited from using official data for any purpose other than in the performance of their official duties for or on behalf of the Agency. Official data is not to be held in personal files or set aside for personal use or benefit.
- (2) Official data is not to be copied or removed from the files of the Agency for release outside the Agency except by those officials authorized through chain of command by the Director of Central Intelligence.
- (3) Any employee who is served with a subpoena which may require the disclosure of official data to a court, the Congress, or a committee of the Congress will promptly inform the General Counsel of the serving of the subpoena, the nature of the information sought, and any circumstances which may bear upon the desirability of making available the official data, so that the General Counsel may advise the Director.
- (4) When not in use, official data must be kept in storage facilities which have been approved by the Director of Security. Consequently, documents which contain official data are not to be taken home or stored in private residences unless the use of an approved, secure facility has been authorized in advance by the Director of Security.
- (5) In addition to the prohibition against unauthorized disclosure of official data outside the Agency, internal disclosure of official data is limited to those employees whose duties require access to it. Employees are not to disclose official data to those who do not need to know it, nor are they to try to obtain official data they do not need to know.

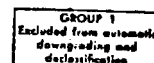
**b. RESPONSIBILITIES**

- (1) Each individual employed by the Central Intelligence Agency is responsible for the secure handling of official data and for protecting it against unauthorized disclosure. Termination of Agency employment will not affect these responsibilities.
- (2) The Director of Personnel is to ensure that all personnel processed through headquarters report to the Office of Security to read this regulation and the statutes referred to in subparagraph c below before entering on duty or separating from the Agency.
- (3) Chiefs of  installations are to ensure that all  personnel not processed through headquarters read this regulation and the statutes referred to in subparagraph c before entering on duty or separating from the Agency.
- (4) Any authorized representative of CIA who negotiates with individuals or organizations for services is to ensure that the appropriate statutory provisions are incorporated in the Secrecy Agreement or contract. The incorporation may be by reference where feasible.

25X1

Revised: 14 November 1969 (508)

CONFIDENTIAL



53

CONFIDENTIAL

HR 

SECURITY

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080027-0

- c. **STATUTORY REFERENCES.** Sections 793, 794, and 798, Title 18 of United States Code prohibit certain activities with respect to defense information and provide penalties for violation. Section 793 provides generally that persons who lose defense information without reporting such loss, or gather or transmit defense information with the intent or with reason to believe such information will be used to the injury of the United States or to the advantage of any foreign nation are subject to a fine of \$10,000 or 10 years imprisonment or both. Section 794 provides generally that persons who communicate or deliver or attempt to communicate or deliver defense information to any foreign government with intent or reason to believe such information will be used to the injury of the United States or to the advantage of a foreign government are subject to imprisonment for not more than 20 years. If this statute is violated during wartime, the punishment is death or imprisonment for not more than 30 years. Both sections 793 and 794 provide like penalties for a conviction of conspiracy to violate either section. Section 798 provides generally that persons who communicate or otherwise make available to an unauthorized person or publisher, or use in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government any classified information relating to cryptography or communications intelligence are subject to a fine of \$10,000 or 20 years imprisonment or both.

CONFIDENTIAL